ABSTRACT

Improvements in intrusion detection are disclosed by providing intrusion event filtering and/or generic attack signature processing. These services may be integrated into a system or server that is the potential target of attack, or alternatively may be implemented in a network device. Filtering may be provided using sensitivity levels and suspicion levels. Generic attack signatures describe relatively broad classes of intrusions. Intrusion detection policy information may be used to direct the actions to be taken upon detecting an attack.